

Configurar o roteamento entre VLANs com switches Catalyst

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Produtos Relacionados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Recomendações](#)

[Verificar](#)

[Catalyst 3850](#)

[Catalyst 4500-A](#)

[Catalyst 4500-B](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o roteamento entre VLANs com switches da série Cisco Catalyst.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como criar VLANs
- Conhecimento de como criar links de tronco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 3850 com Cisco IOS® XE Software Release 16.12.7

- Catalyst 4500 com Cisco IOS® Software Release 03.09.00E

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- Qualquer switch Catalyst 3k/9k e posterior
- Qualquer modelo de switch Catalyst, usado como switch de camada de acesso

Informações de Apoio

Implementando o roteamento entre VLANs, as organizações podem manter os benefícios da segmentação de VLANs enquanto ainda permitem a comunicação necessária entre diferentes partes da rede. Isso é particularmente útil em ambientes de rede complexos onde diferentes departamentos ou serviços precisam interagir com segurança e eficiência. Um exemplo de configuração para o roteamento entre VLANs é configurado em um switch da série Catalyst 3850, com um par de switches da série Catalyst 4500 atuando como switches de Camada 2 (L2) que se conectam diretamente ao Catalyst 3850. O switch Catalyst 3850 tem uma rota padrão para todo o tráfego destinado à Internet. O próximo salto é um roteador Cisco, mas também pode ser qualquer gateway de Internet, como um firewall.

Em uma LAN, as VLANs dividem os dispositivos em domínios de colisão distintos e sub-redes de Camada 3 (L3). Os dispositivos dentro da mesma VLAN podem se comunicar diretamente sem exigir roteamento. No entanto, a comunicação entre dispositivos em VLANs diferentes exige um dispositivo de roteamento.

Os switches de Camada 2 (L2) precisam de um dispositivo de roteamento de L3 para facilitar a comunicação entre VLANs. Esse dispositivo de roteamento pode ser externo ao switch ou integrado em outro módulo dentro do mesmo chassi. Os switches modernos, como o Catalyst 3K/9K, incorporam recursos de roteamento diretamente no switch. Esses switches podem receber um pacote, identificar que ele pertence a uma VLAN diferente e encaminhá-lo à porta apropriada na VLAN de destino.

Um projeto típico de uma rede local segmenta a rede com base no grupo ou função dos dispositivos. Por exemplo, a VLAN de engenharia contém apenas dispositivos relacionados ao departamento de engenharia, enquanto a VLAN de finanças inclui apenas dispositivos

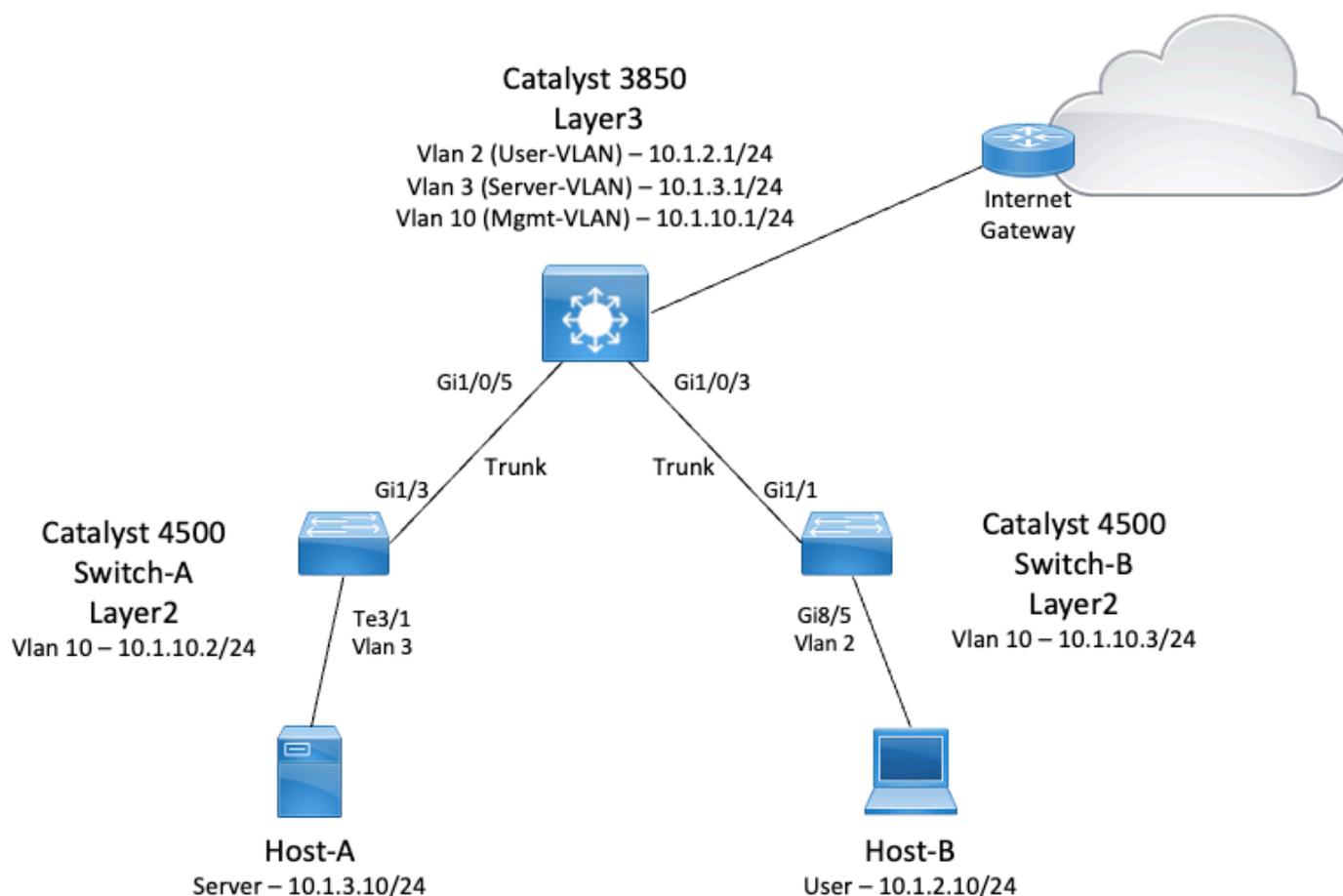
relacionados a finanças. Ativar o roteamento permite que dispositivos em VLANs diferentes se comuniquem sem estar no mesmo domínio de broadcast. Esse projeto de VLAN também oferece uma vantagem adicional: os administradores podem usar listas de acesso para restringir a comunicação entre VLANs. Por exemplo, as listas de acesso podem ser usadas para impedir que dispositivos na VLAN de engenharia acessem dispositivos na VLAN de finanças.

Configurar

Esta seção fornece as informações necessárias para configurar o roteamento entre VLANs conforme descrito neste documento.

 Observação: use as [ferramentas de suporte da Cisco](#) para encontrar mais informações sobre os comandos usados aqui. Somente usuários registrados da Cisco têm acesso a ferramentas como essa e outras informações internas.

Diagrama de Rede



Neste diagrama, o switch Catalyst 3850 fornece a função de roteamento entre VLANs diferentes. O switch Catalyst 3850 pode atuar como um dispositivo L2 com a desativação do roteamento IP. Para fazer com que o switch funcione como um dispositivo L3 e forneça o roteamento entre VLANs, certifique-se de que o roteamento ip esteja habilitado globalmente.

Configurações

As três VLANs seguintes foram definidas para esta configuração:

- VLAN 2 — VLAN de usuário
- VLAN 3 — Servidor-VLAN
- VLAN 10 — VLAN de gerenciamento

Cada servidor e dispositivo de host deve ter seu gateway padrão configurado para o endereço IP da interface VLAN correspondente no Catalyst 3850. Por exemplo, o gateway padrão para servidores é 10.1.3.1. Os switches da camada de acesso, que são o Catalyst 4500, são conectados ao Catalyst 3850 através de links de tronco.

Para o tráfego de Internet, o Catalyst 3850 tem uma rota padrão que aponta para um roteador Cisco, que atua como o gateway de Internet. Consequentemente, todo o tráfego para o qual o Catalyst 3850 não tem uma rota em sua tabela de roteamento é encaminhado ao roteador Cisco para processamento adicional.

Recomendações

- Certifique-se de que a VLAN nativa para um tronco 802.1Q seja a mesma em ambas as extremidades do link de tronco. Se as VLANs nativas forem diferentes, o tráfego nas VLANs nativas não poderá ser transmitido corretamente, podendo causar problemas de conectividade na rede.
- Separe a VLAN de gerenciamento das outras VLANs, conforme ilustrado neste diagrama. Essa separação garante que qualquer tempestade de pacotes ou broadcast na VLAN do usuário ou do servidor não afete o gerenciamento do switch.
- Não use a VLAN 1 para gerenciamento. Todas as portas nos switches Catalyst assumem como padrão a VLAN 1, e todas as portas não configuradas são colocadas na VLAN 1. O uso da VLAN 1 para gerenciamento pode causar problemas em potencial.
- Use uma porta de camada 3 (roteada) para se conectar à porta do gateway padrão. Neste exemplo, um roteador Cisco pode ser substituído por um firewall que se conecta ao roteador de gateway da Internet.
- Este exemplo configura uma rota estática padrão no Catalyst 3850 em direção ao roteador Cisco para acessar a Internet. Essa configuração é ideal se houver apenas uma rota para a Internet. Certifique-se de configurar rotas estáticas, de preferência resumidas, no roteador do gateway para sub-redes alcançáveis pelo Catalyst 3850. Essa etapa é importante porque essa configuração não usa protocolos de roteamento.
- Se você tiver dois switches L3 em sua rede, poderá conectar os switches da camada de acesso aos switches 3850 e executar o Hot Standby Router Protocol (HSRP) entre eles para fornecer redundância de rede.
- Se for necessária largura de banda adicional para as portas de uplink, você poderá configurar EtherChannels, que também fornecerão redundância de link em caso de falha do link.

As configurações em execução dos switches usados na topologia são mostradas a seguir:

 Observação: a configuração do roteador de gateway de Internet não é relevante, portanto, não é abordada neste documento.

- Catalyst 3850
- Catalyst 4500-A
- Catalyst 4500-B

Catalyst 3850

```
<#root>
SW_3850#
show running-config

Building configuration...

Current configuration : 11543 bytes
!
! Last configuration change at 12:16:54 UTC Tue Nov 15 2022
!
version 16.12
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
service call-home
no platform punt-keepalive disable-kernel-core
!

hostname SW_3850

!
!--- IP routing enabled for Inter-VLAN routing.

ip routing

!
!
no ip domain lookup
!
!
login on-success log
!
!
!

vtp mode off

!
!--- Output suppressed.

!--- Configure IEEE 802.1q trunks.
```

!--- Issue the switchport mode trunk command to force the switch port to trunk mode.

```
!  
interface GigabitEthernet1/0/1  
shutdown  
!  
interface GigabitEthernet1/0/2  
shutdown  
!  
interface GigabitEthernet1/0/3 description To_Switch-B switchport mode trunk  
!  
interface GigabitEthernet1/0/4  
no switchport no ip address shutdown  
!  
interface GigabitEthernet1/0/5  
  
description To_Switch-A  
  
switchport mode trunk  
  
!  
interface GigabitEthernet1/0/6  
no switchport  
no ip address  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
!--- This Switch Virtual Interface (SVI) is the default gateway for Users.  
!  
interface Vlan2  
  
description User-SVI  
  
ip address 10.1.2.1 255.255.255.0  
  
!  
!--- This SVI is the default gateway for Servers VLAN.  
!  
interface Vlan3  
  
description Server-SVI  
  
ip address 10.1.3.1 255.255.255.0
```

```
!  
!-- This SVI is the default gateway for other L2 switches management interface.  
!  
interface Vlan10  
  
description Management-SVI  
  
ip address 10.1.10.1 255.255.255.0  
  
!  
!-- This route statement allows the 3850 to send Internet traffic to the Cisco router.  
  
ip route 0.0.0.0 0.0.0.0 10.1.1.2  
  
ip forward-protocol nd  
ip http server  
ip http authentication local  
ip http secure-server  
!  
!  
!  
line con 0  
line vty 5 15  
!  
end
```

 Observação: neste exemplo, o VLAN Trunk Protocol (VTP) foi definido como desativado em todos os switches, com o uso do comando vtp mode off.

<#root>

SW_3850(config)#

vtp mode off

Setting device to VTP Off mode for VLANs.

SW_3850(config)#

vlan 2

SW_3850(config-vlan)#

name User_VLAN

SW_3850(config-vlan)#

exit

SW_3850(config)#

vlan 3

```
SW_3850(config-vlan)#
name Server_VLAN
SW_3850(config-vlan)#
exit
SW_3850(config)#
vlan 10
SW_3850(config-vlan)#
name Mgmt_VLAN
SW_3850(config-vlan)#
exit
SW_3850(config)#
end
```

Catalyst 4500-A

```
<#root>
Switch-A#
show running-config
Building configuration...

Current configuration : 15360 bytes
!
! Last configuration change at 01:06:17 UTC Wed Nov 16 2022
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service compress-config
!
hostname Switch-A
!
no ip domain-lookup
no ip dhcp snooping information option
!
!
login block-for 60 attempts 3 within 60
login delay 1
login quiet-mode access-class testblock
login on-failure log
login on-success log

vtp mode off

!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
!

vlan 3 name Server-VLAN ! vlan 10 name Mgmt-VLAN

!

!--- Output suppressed

!
interface GigabitEthernet1/1
shutdown
!
interface GigabitEthernet1/2
shutdown
!

interface GigabitEthernet1/3 switchport mode trunk

!

!--- Configure Server (Host-A) to be the on the access VLAN 3.

!

interface TenGigabitEthernet3/1 switchport access vlan 3 switchport mode access

!
interface TenGigabitEthernet3/2
shutdown
!
interface TenGigabitEthernet3/3
!
interface TenGigabitEthernet3/4
!

!--- Output suppressed.
!--- IP address on VLAN 10 manages this switch.

!
interface Vlan1
no ip address
!

interface Vlan10 ip address 10.1.10.2 255.255.255.0

!
ip forward-protocol nd
ip http server
ip http banner
ip http authentication local
!

!--- Configure the default gateway so that the switch is reachable from other !--- VLANs/subnets. The gateway points to the VLAN 10 interface on the 3850

ip default-gateway 10.1.10.1
ip forward-protocol nd
ip http server
ip http banner
```

```
ip http authentication local
!  
!  
line con 0  
stopbits 1  
line vty 0 4  
logging synchronous  
transport input all  
line vty 5 15  
logging synchronous  
transport input all  
!  
end
```

Catalyst 4500-B

```
<#root>
```

```
Switch-B#
```

```
show running-config
```

```
Building configuration...
```

```
Current configuration : 6841 bytes
```

```
!  
! Last configuration change at 10:44:33 UTC Tue Nov 15 2022  
!
```

```
version 15.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!
```

```
hostname Switch-B
```

```
!  
boot-start-marker  
boot system bootflash:cat4500es8-universal.SPA.03.11.06.E.152-7.E6.bin  
boot-end-marker  
!
```

```
vrf definition mgmtVrf
```

```
!  
address-family ipv4  
exit-address-family  
!  
address-family ipv6  
exit-address-family  
!
```

```
no aaa new-model  
hw-module module 7 mode 1
```

```
!  
!  
!  
!
```

```
!  
!  
!  
!  
!  
vtp mode off  
  
!  
! spanning-tree mode pvst spanning-tree extend system-id !  
  
vlan 2  
name User-VLAN  
!  
vlan 10 name  
Mgmt-VLAN  
  
!  
!  
  
interface GigabitEthernet1/1 switchport mode trunk  
  
!  
interface GigabitEthernet1/2  
!  
interface GigabitEthernet1/3  
shutdown  
!  
interface GigabitEthernet1/4  
shutdown  
!  
  
!--- Output suppressed.  
!--- Configure User (Host-B) in VLAN 2.  
  
!  
  
interface GigabitEthernet8/5 switchport access vlan 2 switchport mode access  
  
!  
  
!--- Configure the management IP address in VLAN 10.  
!  
interface Vlan1  
no ip address  
!  
  
interface Vlan10 ip address 10.1.10.3 255.255.255.0  
  
!  
  
!--- Define the default route so that the switch is reachable.  
!  
  
ip default-gateway 10.1.10.1  
  
ip forward-protocol nd  
ip http server  
ip http banner  
ip http authentication local
```

```
!  
!  
line con 0  
  stopbits 1  
line vty 0 4  
  login  
  transport input none  
!  
!  
end
```

Verificar

Em seguida, você encontrará uma lista de comandos essenciais que podem ser utilizados para verificar o status dos dispositivos e confirmar se a configuração está funcionando corretamente:

show vtp status - Este comando exibe o status do VLAN Trunking Protocol (VTP) no switch. Ele fornece informações sobre a versão do VTP, o nome do domínio, o modo (servidor, cliente ou transparente) e o número de VLANs existentes. Isso é útil para verificar a configuração do VTP e garantir informações consistentes de VLAN na rede.

show interfaces trunk - Esse comando mostra o status das portas de tronco no switch. Ele fornece detalhes sobre quais interfaces são configuradas como troncos, o tipo de encapsulamento (por exemplo, 802.1Q) e as VLANs permitidas em cada tronco. Isso é essencial para solucionar problemas de conectividade de VLAN e garantir a configuração apropriada do tronco.

show ip route - Este comando exibe a tabela de roteamento IP do switch. Ele lista todas as rotas conhecidas, incluindo redes diretamente conectadas, rotas estáticas e rotas aprendidas por protocolos de roteamento dinâmico. Isso é crucial para verificar os caminhos de roteamento e garantir que o switch possa acessar todas as redes necessárias.

show ip cef - Este comando mostra a saída do Cisco Express Forwarding (CEF). Ele fornece informações sobre as entradas CEF, incluindo os endereços do próximo salto e as interfaces associadas. Isso é útil para solucionar problemas de encaminhamento e garantir o processamento eficiente de pacotes.



Observação: a ferramenta [Cisco CLI Analyzer](#) pode ajudar a solucionar problemas e verificar a integridade geral do software suportado pela Cisco com este cliente SSH inteligente que usa ferramentas e conhecimento TAC integrados.

 Observação: para obter detalhes sobre comandos CLI, consulte os Guias de Referência de Comandos para uma plataforma de switching específica.

 Observação: somente usuários registrados da Cisco têm acesso a ferramentas como essa e outras informações internas.

Catalyst 3850

<#root>

SW_3850#

H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is 10.100.100.2 to network 0.0.0.0

```
s* 0.0.0.0/0 [1/0] via 10.100.100.2
```

10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

```
C 10.1.2.0/24 is directly connected, Vlan2
L 10.1.2.1/32 is directly connected, Vlan2
C 10.1.3.0/24 is directly connected, Vlan3
L 10.1.3.1/32 is directly connected, Vlan3
C 10.1.10.0/24 is directly connected, Vlan10
L 10.1.10.1/32 is directly connected, Vlan10
C 10.100.100.0/24 is directly connected, GigabitEthernet1/0/2
L 10.100.100.1/32 is directly connected, GigabitEthernet1/0/2
```

Catalyst 4500-A

```
<#root>
```

```
Switch-A#
```

```
show vtp status
```

```
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : cisco.com
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : 6400.f13e.dc40
Configuration last modified by 10.1.10.2 at 0-0-00 00:00:00
```

```
Feature VLAN:
```

```
-----
```

```
VTP Operating Mode : Off
```

```
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 32
Configuration Revision          : 0
MD5 digest                      : 0x0B 0x61 0x4F 0x9B 0xCD 0x1B 0x37 0x55
                                0xAB 0x0C 0xC1 0x4B 0xF8 0xDE 0x33 0xB3
```

```
<#root>
```

```
Switch-A#
```

```
show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gi1/3	on	802.1q	trunking	1

Port Vlans allowed on trunk

Gi1/3 1-4094

Port Vlans allowed and active in management domain

Gi1/3 1,3,10

Port Vlans in spanning tree forwarding state and not pruned

Gi1/3 1,3,10

Catalyst 4500-B

<#root>

Switch-B#

show vtp status

```
VTP Version capable      : 1 to 3
VTP version running     : 1
VTP Domain Name         :
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : 6c20.5606.3540
Configuration last modified by 10.1.10.3 at 11-15-22 10:42:29
```

Feature VLAN:

VTP Operating Mode : Off

```
Maximum VLANs supported locally : 1005
Number of existing VLANs       : 7
Configuration Revision         : 0
MD5 digest                    : 0xEC 0xB4 0x8D 0x46 0x94 0x95 0xE0 0x8F
                               0xEE 0x1E 0xC7 0x9F 0x26 0x88 0x49 0x9F
```

<#root>

Switch-B#

show interfaces trunk

```
Port      Mode           Encapsulation  Status        Native vlan
Gi1/1 on 802.1q trunking 1
```

Port Vlans allowed on trunk

Gi1/1 1-4094

Port Vlans allowed and active in management domain

Gi1/1 1-2,10

Port Vlans in spanning tree forwarding state and not pruned

Gi1/1 1-2,10

Troubleshooting

1. Problemas de Ping na Mesma VLAN

- Se você não puder fazer ping de dispositivos dentro da mesma VLAN, verifique a atribuição de VLAN das portas origem e destino para garantir que eles estejam na mesma VLAN.
- Para verificar a atribuição de VLAN, use o comando `show interface status`.
- Use o comando `show mac address-table` para verificar se o switch L2 está aprendendo o endereço MAC de cada dispositivo na VLAN apropriada.

2. Problemas de Ping em Switches Diferentes

- Se a origem e o destino estiverem em switches diferentes, assegure-se de que os troncos estejam configurados corretamente. Use o comando `show interfaces trunk` para verificar a configuração.
- Verifique se a VLAN nativa corresponde em ambos os lados do link de tronco e se a máscara de sub-rede corresponde entre os dispositivos origem e destino.

3. Problemas de Ping Entre VLANs Diferentes

- Se você não conseguir fazer ping em dispositivos em VLANs diferentes, assegure-se de que você possa fazer ping no respectivo gateway padrão (consulte a Etapa 1).
- Verifique se o gateway padrão do dispositivo aponta para o endereço IP da interface VLAN correto e se a máscara de sub-rede corresponde.

4. Problemas de conectividade com a Internet

- Se você não conseguir acessar a Internet, verifique se a rota padrão no Catalyst 3850 aponta para o endereço IP correto e se o endereço de sub-rede corresponde ao roteador de gateway de Internet.
- Certifique-se de que o switch L3 (3850 neste cenário) seja capaz de fazer ping no gateway de Internet.
- Para verificar, use o comando `show ip cef <prefix>` para identificar se ele aponta para a interface correta.
- Certifique-se de que o roteador do gateway de Internet tenha rotas para a Internet e para as redes internas.

Informações Relacionadas

- [Configurar o roteamento entre VLANs usando um roteador externo](#)

- [Criar VLANs Ethernet nos switches Catalyst](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.